

JHT:hcs

AO 106 (Rev. 04/10) Application for a Search Warrant

2021R00210

UNITED STATES DISTRICT COURT

for the
District of MinnesotaIN THE MATTER OF THE SEARCH OF THE
SUBJECT DEVICES DESCRIBED IN
ATTACHMENT A CURRENTLY IN FBI
CUSTODY

Case No. 24-mj-382 (ECW)

APPLICATION FOR A SEARCH WARRANT

I, Travis Wilmer, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A, incorporated here

located in the State and District of Minnesota, there is now concealed:

See Attachment B, incorporated here

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code SectionOffense Description

Title 18, United States Code, Section 201
 Title 18, United States Code, Section 1503

Bribery of jurors
 Influencing or injuring officer or juror generally

The application is based on these facts:

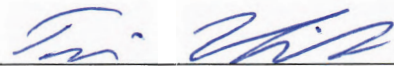
See Affidavit, incorporated here

☒ Continued on the attached sheet.

SUBSCRIBED and SWORN before me by reliable
 electronic means (FaceTime, Zoom and/or email)
 pursuant to Fed. R. Crim. P. 41(d)(3)

Date: June 3, 2024

City and State: St. Paul, MN



Applicant's Signature

Travis Wilmer, Special Agent
 FBI

Printed Name and Title



Judge's Signature

The Honorable Elizabeth Cowan Wright
 United States Magistrate Judge

Printed Name and Title

STATE OF MINNESOTA)
)
COUNTY OF RAMSEY) ss. AFFIDAVIT OF TRAVIS WILMER

Your affiant, Travis Wilmer, being duly sworn, does state the following is true and correct to the best of his knowledge and belief:

1. I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since November 8, 2021.

2. As a Special Agent, my primary duties and responsibilities consist of conducting investigations of individuals and businesses for possible violations of federal laws. I am presently assigned to the FBI's Minneapolis, Minnesota field office where I am a member of the Civil Rights and Public Corruption Squad.

3. During my employment as a Special Agent, I have conducted and participated in investigations of varying degrees involving mail fraud, wire fraud, fraud against the government, money laundering, and other criminal acts, including criminal schemes where individuals misappropriate money from the investing public. Furthermore, in the course of my training and experience, I have become familiar with the types of records businesses typically maintain in the course of their regular activity, including ledgers, journals, invoices, receipts, and bank documents. I am also familiar with the investigation of obstruction of justice, bribery, and other tampering offenses. I am aware that individuals who commit these offenses—and notably when they conspire with others to commit these offenses—often use electronic communications in the course of their crimes. Further, I know that when large sums

of money, and in particular cash, are used to commit crimes, including bribery offenses, communications stored in cellular telephones, including bank records, may reveal the source of those funds.

4. This affidavit is submitted in support of an application for warrants to search:

a. cellular telephone(s) in the possession of Abdiaziz Shafii Farah, Mohamed Jama Ismail, Abdimajid Mohamed Nur, Said Shafii Farah, Abdiwahab Maalim Aftin, Mukhtar Mohamed Shariff, and Hayat Mohamed Nur as further described in Attachment A (the “**Subject Devices**”), for evidence and fruits of violations of Title 18, United States Code, Sections 201 (bribery of jurors) and 1503 (Influencing or injuring officer or juror generally).

5. This affidavit is based on my personal knowledge, interviews of witnesses, physical surveillance, information received from other law enforcement agents, my experience and training, and the experience of other agents. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a search warrant for the Subject Devices, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and fruits of violations of Title 18, United States Code, Sections 201 and 1503 are located on the Subject Devices.

I. OVERVIEW

6. In recent years, individuals and companies in Minnesota have engaged in a large-scale scheme to fraudulently obtain and misappropriate funds from federal

child nutrition programs. The scheme was carried out by individuals who owned and operated companies purportedly in the business of providing federally funded free meals to underprivileged children and adults, including during the global Covid-19 pandemic. The companies and their owners received tens of millions of dollars in federal funds for use in providing nutritious meals to underprivileged children and adults. Very little of this money was used to feed children. Instead, the participants in the scheme misappropriated the money and used it to purchase real estate, cars, and other luxury items. To date, the conspirators have stolen millions of dollars in federal funds.

II. BACKGROUND

A. The Federal Child Nutrition Programs

7. This warrant relates to an ongoing investigation into a scheme to defraud United States Department of Agriculture (USDA) programs that provide federal funding to nutrition programs for children and low-income individuals across the nation. The USDA operates two such programs—the Summer Food Service Program and the Child and Adult Care Food Program.

8. The Summer Food Service Program (SFSP) is a federal program designed to ensure that low-income children continue to receive nutritious meals when school is not in session.

9. The Child and Adult Care Food Program (CACFP) is a federal program that provides reimbursements for nutritious meals and snacks to eligible children and adults who are enrolled for care at participating child care centers, day care homes, and adult day care centers. CACFP also provides reimbursements for meals

served to children participating in afterschool care programs or residing in emergency shelters and adults over the age of 60 or living with a disability and enrolled in day care facilities.

10. The Summer Food Service Program and Child and Adult Care Food Program (together, the “Federal Child Nutrition Programs”) operate throughout the United States. The USDA’s Food and Nutrition Service administers the programs at the national and regional levels by disbursing federal funds to state governments, which provide oversight over the Federal Child Nutrition Programs.

11. Within each state, the Federal Child Nutrition Programs are administered by the state department of education or an alternate state-designated agency. In Minnesota, the programs are administered by the Minnesota Department of Education (MDE).

12. Locally, meals funded by the Federal Child Nutrition Program are served at sites such as schools or daycare centers (“Sites”). Each Site must be sponsored by a public or private non-profit organization that is authorized to participate in the Federal Child Nutrition Programs (“Sponsors”). Sponsors seeking to participate in the Federal Child Nutrition Programs are required to submit an application to the MDE for approval for each site from which they intend to operate Federal Child Nutrition Programs. Sponsors are responsible for monitoring each of their sites and preparing reimbursement claims for their sites.

13. Federal Child Nutrition Program funds are supposed to be used to provide nutritious meals and food to children and low-income individuals. *See* 7

C.F.R. § 225.15(a)(4) (“All Program reimbursement funds must be used solely for the conduct of the nonprofit food service operation.”).

14. Historically, the Federal Child Nutrition Program has generally functioned through the provision of meals to children involved in educational-based programs or activities. During the Covid-19 pandemic, however, the USDA waived some of the standard requirements for participation in the Federal Child Nutrition Program. Among other things, USDA allowed for-profit restaurants to participate in the program. It also allowed for off-site food distribution to children outside of educational programs. At the same time, the state government’s stay-at-home order and telework policies interfered with the ability to oversee the program. According to MDE officials, this left the program vulnerable to fraud and abuse.

B. Seven Defendants Proceeded to Trial on April 22, 2024

15. To date, 70 defendants have been charged for their roles in this fraud scheme. On April 22, 2024, a trial of seven of these defendants—Abdiaziz Shafii Farah, Mohamed Jama Ismail, Abdimajid Mohamed Nur, Said Shafii Farah, Abdiwahab Maalim Aftin, Mukhtar Mohamed Shariff, and Hayat Mohamed Nur—commenced in the District of Minnesota before The Honorable Nancy Brasel. *United States v. Abdiaziz Farah, et al.*, 22-cr-124 (NEB).

16. The first week of trial, a jury was selected and seated. One of the jurors selected to serve in the trial was Juror #52. While the general public did not have access to the personal information of jurors, counsel for the government, counsel for the defense, and the seven defendants on trial had access to this information.

17. The trial is ongoing, currently in its seventh week. On Friday, May 31, 2024, half of the closing arguments were completed. Three remaining defense closing arguments, as well as the government's rebuttal argument, were set to occur today, Monday June 3, 2024. The Court and parties anticipated that the jury would begin deliberations today.

C. Bribe Payment Delivered to Juror #52's Home

18. On June 2, 2024—the night before trial was set to conclude—at approximately 8:50pm, a woman approached the home of Juror #52 and rang the doorbell. Juror #52 was not home at the time. A relative of the juror answered the door. The relative described the woman as a black woman, possibly Somali, with an accent, wearing a long black dress. The woman handed a gift bag to the relative and said it was a present for Juror #52. The woman used Juror #52's first name. The woman told the relative to tell Juror #52 to say not guilty tomorrow and there would be more of that present tomorrow. After the woman left, the relative looked in the gift bag and saw it contained a substantial amount of cash. When Juror #52 returned home and was told of the encounter, Juror #52 immediately called 911 to report the incident. The Spring Lake Park Police responded. Juror #52 gave the bag of cash to the Spring Lake Park Police. The bag of cash contained 100-, 50-, and 20-dollar bills, totaling approximately \$120,000. This morning, the FBI interviewed Juror #52 and took custody of the bag of cash from the Spring Lake Park Police.





D. Court Proceedings on June 3, 2024

19. This morning, the Court, counsel for the government, and counsel for the defendants learned of the attempt to bribe Juror #52. At this morning's Court proceedings, among other things, the government moved to take custody of the cell

phones of the seven defendants—all of whom would have had access to Juror #52’s identifying information—to effectively “freeze” the scene. The Court ordered that the defendants surrender their cell phones to law enforcement. The seven surrendered cell phones (the “Subject Devices”) are currently in the custody of the FBI. The Subject Devices, as described in Attachment A, are as follows:

- a. Defendant Abdiaziz Farah: Black Apple iPhone in smooth black rubberized case with the Apple logo on the back of the case;
- b. Defendant Mohamed Ismail: Blue Apple iPhone in smooth case with semi-transparent back, black edges, and blueish-chrome buttons;
- c. Defendant Abdimajid Nur: Gray Apple iPhone in smooth black leatherette case with the Apple logo on the back of case;
- d. Defendant Said Farah: Blue Apple iPhone in smooth clear transparent case with hard back and flexible sides;
- e. Defendant Abdiwahab Aftin: White Apple iPhone in black textured case with brown paper showing through cutout in rear of case;
- f. Defendant Mukhtar Shariff: Blueish Gray Apple iPhone in smooth black case with the words “Cord King” and “Designed in Paris France” inscribed on the back inside of the case; and
- g. Defendant Hayat Nur: Light Blue Apple iPhone in smooth case with semi-transparent back and chrome edges and buttons.

III. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based upon my knowledge, training, experience, and the experience of other law enforcement personnel, I know that computer hardware and computer

software may be utilized to store records which include, but are not limited to: those relating to business activities, criminal activities, associate names and addresses, victims' names, addresses, and images, the identity and location of assets illegally gained through criminal activity, and other information related to criminal activity.

21. With respect to the particular crimes alleged, I am aware that communications with others, including others involved in criminal activities, are often stored on mobile devices like cell phones. Here, it is highly likely that someone with access to the juror's personal information was conspiring with, at minimum, the woman who delivered the \$120,000 bribe. Indeed, in this case in particular, these defendants and others conspirators used electronic communication, including text messages and e-mails, to communicate about their illicit activities.

22. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Devices. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Biometric Access to Devices(s).* This warrant permits law enforcement agents to obtain from the persons of Abdiaziz Shafii Farah, Mohamed Jama Ismail, Abdimajid Mohamed Nur, Said Shafii Farah, Abdiwahab Maalim Aftin, Mukhtar Mohamed Shariff, and Hayat Mohamed Nur the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned persons' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

26. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer

a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

27. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

28. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

29. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

30. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

31. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

32. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

33. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the

fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the **Subject Devices**; (2) hold the **Subject Devices** in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the **Subject Devices** in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

34. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

IV. CONCLUSION


35. Based on the facts set forth above, and based on my training, experience, knowledge, and the aforementioned facts of this investigation, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 201 and 1503, as described in Attachment B, can be found on the Subject Devices, as further described in Attachment A.

Respectfully submitted,



FBI Special Agent Travis Wilmer

SUBSCRIBED and SWORN before me by reliable
electronic means (FaceTime, Zoom and/or email)
pursuant to Fed. R. Crim. P. 41(d)(3) on
June 3, 2024


The Honorable Elizabeth Cowan Wright
United States Magistrate Judge

ATTACHMENT A
(List of Items to be Searched)

The property to be searched are cellular phones found in the possession of Abdiaziz Shafii Farah, Mohamed Jama Ismail, Abdimajid Mohamed Nur, Said Shafii Farah, Abdiwahab Maalim Aftin, Mukhtar Mohamed Shariff, and Hayat Mohamed Nur, currently in the possession of the FBI, as follows:

- a. Defendant Abdiaziz Farah: Black Apple iPhone in smooth black rubberized case with the Apple logo on the back of the case;
- b. Defendant Mohamed Ismail: Blue Apple iPhone in smooth case with semi-transparent back, black edges, and blueish-chrome buttons;
- c. Defendant Abdimajid Nur: Gray Apple iPhone in smooth black leatherette case with the Apple logo on the back of case;
- d. Defendant Said Farah: Blue Apple iPhone in smooth clear transparent case with hard back and flexible sides;
- e. Defendant Abdiwahab Aftin: White Apple iPhone in black textured case with brown paper showing through cutout in rear of case;
- f. Defendant Mukhtar Shariff: Blueish Gray Apple iPhone in smooth black case with the words "Cord King" and "Designed in Paris France" inscribed on the back inside of the case; and
- g. Defendant Hayat Nur: Light Blue Apple iPhone in smooth case with semi-transparent back and chrome edges and buttons.

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
(List of Items to be Seized)

Items to be seized include all evidence of violations of Title 18, United States Code, Sections 201 (bribery of jurors) and 1503 (influencing a juror) for the time period of April 22, 2024 to the present, related to a scheme to fraudulently obtain, launder, and misappropriate federal child nutrition program funds, including the following:

1. All records or communications pertaining to potential witnesses or jurors in the ongoing trial;
2. All records or communications pertaining to attempts to obstruct justice in the ongoing trial;
3. All records or communications, including financial records, that concern obtaining, transferring, or holding large sums of money, including cash;
4. With respect to any digital-device containing evidence falling within the scope of the foregoing categories of items to be seized:
 - a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
 - b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. As used herein, the terms "records," "documents," "programs," "applications," and "materials" includes records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.